

David Kirby

ECE 595: Advanced Technical Cybersecurity

Spring, 2022

Virtual Environment

```
david@ubuntu:~/Documents/A1$ gcc -g3 -o f2 function.c
david@ubuntu:~/Documents/A1$ gdb f2
pwndbg: loaded 191 commands. Type pwndbg [filter] for a list.
pwndbg: created $rebase, $ida gdb functions (can be used with print/break)
Reading symbols from f2...
pwndbg> b function_2
Breakpoint 1 at 0x1171: file function.c, line 7.
pwndbg> r
Starting program: /home/david/Documents/A1/f2
function 1, cnt = 0
function 1, cnt = 1
function 1, cnt = 2
function 1, cnt = 3
function 1, cnt = 4

Breakpoint 1, function_2 (x=4) at function.c:7
7      void function_2(int x){
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[ REGISTERS ]
RAX 0x0
RBX 0x555555551f0 ( __libc_csu_init) ← endbr64
RCX 0x0
RDX 0x0
RDI 0x0
RSI 0x5555555592a0 ← 'function 1, cnt = 4\n'
R8 0x0
R9 0x14
R10 0x555555556018 ← 0x6974636e7566000a /* '\n' */
R11 0x246
R12 0x555555555060 ( _start) ← endbr64
R13 0x7fffffffdd0 ← 0x1
R14 0x0
R15 0x0
RBP 0x7fffffffdd00 ← 0x0
RSP 0x7fffffffddce8 → 0x555555551d5 (main+60) ← add dword ptr [rbp - 4], 1
RIP 0x55555555171 (function_2) ← endbr64
[ DISASM ]
> 0x55555555171 <function_2> endbr64
0x55555555175 <function_2+4> push rbp
0x55555555176 <function_2+5> mov rbp, rsp
0x55555555179 <function_2+8> sub rsp, 0x10
0x5555555517d <function_2+12> mov dword ptr [rbp - 4], edi
0x55555555180 <function_2+15> mov eax, dword ptr [rbp - 4]
0x55555555183 <function_2+18> mov esi, eax
0x55555555185 <function_2+20> lea rdi, [rip + 0xe8e]
0x5555555518c <function_2+27> mov eax, 0
0x55555555191 <function_2+32> call printf@plt <printf@plt>
0x55555555196 <function_2+37> nop
[ SOURCE (CODE) ]
In file: /home/david/Documents/A1/function.c
2
3 void function_1(int x){
4     printf("function 1, cnt = %d\n", x);
5 }
6
7 void function_2(int x){
8     printf("function 2, cnt = %d\n", x);
9 }
10
11 int main() {
12     int i;
[ STACK ]
00:0000 rsp 0x7fffffffddce8 → 0x555555551d5 (main+60) ← add dword ptr [rbp - 4], 1
01:0008 0x7fffffffddcf0 → 0x7fffffffdd0 ← 0x1
02:0010 0x7fffffffddcf8 ← 0x5
03:0018 rbp 0x7fffffffdd00 ← 0x0
04:0020 0x7fffffffdd08 → 0x7ffff7de60b3 ( __libc_start_main+243) ← mov edi, eax
05:0028 0x7fffffffdd10 → 0x7ffff7ffc620 ( _rld_global_ro) ← 0x50d1300000000
06:0030 0x7fffffffdd18 → 0x7fffffffddfb → 0x7fffffe17c ← '/home/david/Documents/A1/f2'
07:0038 0x7fffffffdd20 ← 0x100000000
[ BACKTRACE ]
> f 0 0x55555555171 function_2
f 1 0x555555551d5 main+60
f 2 0x7ffff7de60b3 __libc_start_main+243
pwndbg> □
```

FIGURE 1: DEBUGGING USING GDB AND PWNDBG ON UBUNTU.